March 1, 2018

Chris Nierman
(202) 457-8815
cnierman@gci.com

VIA ELECTRONIC FILING

Ms. Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street SW
Washington, D.C. 20554

Re: EB Docket No. 06-36
Annual CPNI Certification for 2017

Dear Ms. Dortch:

Pursuant to Section 64.2009(e) of the Commission's rules, attached is the 2017 CPNI certification with accompanying statement for GCI Communication Corp. (GCI).

Sincerely,

Chris Nierman
Senior Counsel, Federal Affairs
General Communication, Inc.
1900 L St., N.W., Suite 700
Washington, DC 20036
(202) 457-8815

Annual 47 C.F.R. § 64.2009(e) CPNI Certification

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2017

Date filed: March 1, 2018

Name of company covered by this certification: GCI Communication Corp.

Form 499 Filer ID: 807630 GCI Communication Corp.

Name of signatory: Chris Nierman

Title of signatory: Senior Counsel, Federal Affairs

I, Chris Nierman, certify that I am an authorized employee of the parent company named above, and acting as an agent of the company, that I have personal knowledge that, as detailed herein, the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See* 47 C.F.R. § 64.2001 *et seq*.

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements set forth in part 64.2001 *et seq.* of the Commission's rules.

The company has not taken any actions (proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year. Companies must report on any information that they have with respect to the processes pretexters are using to attempt to access CPNI , and what steps companies are taking to protect CPNI.

The company received one customer complaint in 2017 concerning the unauthorized release of CPNI and made the appropriate notifications pursuant to part 64.2011 of the Commission's rules. A summary of the complaint is included below in Section 6 of the Statement of CPNI Compliance Procedures.

_____

Chris Nierman
Senior Counsel, Federal Affairs
General Communication, Inc.
1900 L St., N.W., Suite 700
Washington, DC 20036
(202) 457-8815

STATEMENT OF CPNI COMPLIANCE PROCEDURES

The following applies to GCI Communication Corp. ("GCI" or "Company"). GCI follows the CPNI Compliance Procedures for all local, long distance, and wireless services, regardless of the technology used to provision the service.

1. *Notice to customers (Section 64.2008).* GCI maintains a notice of CPNI rights to consumers available via website at www.gci.com. This notice is continually available. In addition, GCI issues written notice to customers at least every two years, and issues a notice to new customers in their first billing cycle. Both forms of notice, on website and written, are reviewed periodically, but in no event less than annually, to ensure compliance with current law and regulations. Records of notification are maintained for at least one year.

2. *Customer approvals (Sections 64.2005, 2007, 2008, and 2009(a) & (f)).* To target a customer for sale of a product outside of the existing subscription basket, GCI ensures prior customer approval via opt-out mechanism or one-time approval for in-bound calls. GCI does not use the opt-in mechanism because there is no instance in which it provides CPNI to third party vendors, joint venture partners, or independent contractors for the purpose of marketing communications-related services, or to affiliated entities that provide non-communications-related services.

   Opt-out – GCI allows customers to exercise opt-out rights via website and periodic mailings. The website directs customers who wish to decline approval for use of CPNI to a GCI e-mail box. Any responses are recorded in the customer's account records. Company also provides notice to its customers at least every two years as required by Section 64.2008(d)(2). GCI records responses in each customer account, including the dates when the last notice was mailed and accordingly, the date upon which approval could be deemed given. The CPNI opt-out process is initiated upon the establishment of any new account.

   Employees are trained to check the CPNI designation before accessing or using CPNI data. In addition, if an employee has any reason to believe the opt-out notice has failed for some reason, then he or she is trained to notify a supervisor immediately. Any opt-out notification failure is to be reported to the Compliance Officer (as defined below) for review and further action as necessary in compliance with Section 64.2009(f).

   One-time approval/in-bound calls – in cases where the opt-out process has not been completed or where it has been exercised, customer approval must be obtained for the duration of an in-bound call before CPNI is accessed or used. Record of customer approval is retained in the customer records for at least one year. Customer service employees are trained to seek such approval by following a script approved for compliance with Section 64.2008(f).

All continuing customer approvals or declinations are electronically recorded to ensure that the status of a customer's CPNI approval can be clearly established prior to the use of CPNI.

3. *Training and Disciplinary Processes (Sections 64.2009(b) and 64.2010(a)).* All Company employees are required to review annually the Company's confidentiality policies, which include a description of and requirements for compliance with CPNI requirements and are available at all times on the Company's intranet. These policies establish disciplinary procedures in the event of any violation, prohibit any deviation from compliance, and direct employees with any questions about CPNI compliance to raise those questions with the Regulatory Department. Disciplinary action includes termination. In addition, only employees who require access to customer data in order to perform their assigned duties will be granted access to computer screens or databases that include CPNI. Decisions about employee access to CPNI will be made on a case-by-case basis by the authorized manager, taking into account the requirements of the specific position at the time of initial employment and thereafter with any change in position or duties.

   Customer service representatives with access to CPNI receive additional training through the course of their employment to ensure that the required notice and prior approvals are secured before any access to or use of CPNI and to ensure that such representatives can detect, discover, and therefore protect against attempts to gain unauthorized access to CPNI, including pretexting. The training is available on the Company intranet and as part of the training handbook in paper form.

4. *Marketing and Sales Campaigns (Sections 64.2009(c) & (d)).* Company has instituted standard operating procedures for document retention and marketing plan approval. Designated marketing and sales managers are required to keep records of those campaigns that use CPNI for a minimum of one year, including information identifying each campaign, the CPNI that was used in the campaign, and what products and services were offered as part of the campaign. Procedures are also in place to document when such information is disclosed to third parties, but such information has traditionally been limited to subscriber list information. In addition, all marketing plans must include a CPNI compliance review, approved by the designated supervisor.

5. *Safeguards on the disclosure of CPNI (Section 64.2010).* Customer service representatives are trained to properly authenticate a customer prior to disclosing CPNI, with the exclusion of call detail record, over the phone. Customers may authenticate themselves using a PIN, password, customer-established secret question/secret answer, and other non-biographical account information.

   Company does not provide call detail information over the telephone, based on customer-initiated contact. Customers requesting call detail information by customer-initiated telephone call will be provided with call detail information only by sending it to the customer's address of record or by calling the customer at the telephone number of record. If a customer is able to provide call detail information to the Company during a

customer-initiated call without the Company's assistance, the Company will discuss the call detail information provided by the customer.

Further to its efforts to safeguard against the unauthorized disclosure of CPNI, Company has implemented guidelines to ensure that personnel with access to CPNI are limited to those individuals who require such access to perform their assigned duties. Access is available only through an affirmative managerial grant of permission.

Company has implemented on-line password protection for its on-line account access services, whereby a customer will be authenticated via a unique PIN, without the use of readily available biographical information, or account information, for the purpose of securing a password. The password is required for accessing CPNI online for a telecommunications service account. Business customers subscribing to services for which GCI has bound itself contractually to alternative authentication regimes may waive the use of PIN authentication.

Company's practices require that CPNI is not disclosed to a customer at a Company retail location unless the customer first presents a valid photo ID matching the customer's account information.

GCI issues customer notification of a change or creation of an address of record, the e-mail of record, security word, PIN or password of record immediately upon confirmation of the address of record. The notification is sent to the last postal or email address of record, or (if neither of the former is available or has not been associated with the customer's account for at least 30 days) via voice mail to the telephone number of record. GCI applies the same procedures to business customers as residential customers. The notice does not reveal the changed information.

6. *Notification of CPNI security breaches (Section 64.2011).* Company's operating procedures require notification of relevant law enforcement agencies and customers in accordance with FCC rules in the event of a breach of CPNI.

Upon notification by personnel to the Senior Counsel, Federal Affairs of a suspected breach, an inquiry will be conducted to determine whether a breach occurred.

All records of such recovered breaches shall be maintained in GCI's Washington, D.C. office, and retained for a period of no less than two years. These records will include, where available, dates of discovery and notification, a detailed description of the CPNI that was the subject of the breach, and the circumstances of the breach.

Company has not taken any action against data brokers.

GCI received one customer complaint in 2017 concerning the unauthorized release of CPNI. In that circumstance, a Company customer service representative (CSR) forwarded a wireless customer's complaint about poor service to the CSR's friend who worked for the same employer as the customer, thus inappropriately sharing the fact that

the customer was a GCI wireless subscriber. The CSR was reprimanded according to GCI's policies on maintaining the confidentiality of customer information. Pursuant to part 64.2011 of the Commission's rules, GCI reported the incident within seven business days of reasonable determination of the breach to the FBI and U.S. Secret Service and ensured notice to the customer. The FBI and the U.S. Secret Service informed GCI that they would not be taking any action based on GCI's report.

7. *Customers for whom CPNI is not used.* GCI does not use CPNI for marketing purposes with respect to its customers of Alaska Wireless-brand services, and GCI does not share CPNI of these customers internally or with any other company for marketing purposes, including affiliates, joint ventures, or independent contractors. CPNI is not available to customers via telephone or on-line access. Such customers are located in a geographically segregated area and served by separately established systems by a predecessor entity acquired by GCI in June 2008. Any future use of CPNI with respect to these customers will follow established Company procedures.

8. *Compliance Certification (Sections 64.2009(e) & (f)).* The Senior Counsel, Federal Affairs for GCI is designated to issue the required compliance certificate annually (the "Certifying Officer"), for filing annually with the Enforcement Bureau on or before March 1 in EB Docket No. 06-36, for data pertaining to the previous calendar year. The Certifying Officer is responsible for reviewing these CPNI Compliance Procedures to ensure timely and continuing compliance with relevant legal and/or regulatory changes. In addition, the Certifying Officer will ensure that any notification of failure of the opt-out mechanism to work properly is submitted to the Commission within five business days of such occurrence, in accordance with the procedures set forth in Section 64.2009(f).